

# Практические работы 5-0..5-4. Конфигурирование серверов

## Практическая работа 5-0. Настраиваем WEB сервер

Топология приведена на рис 5.1.

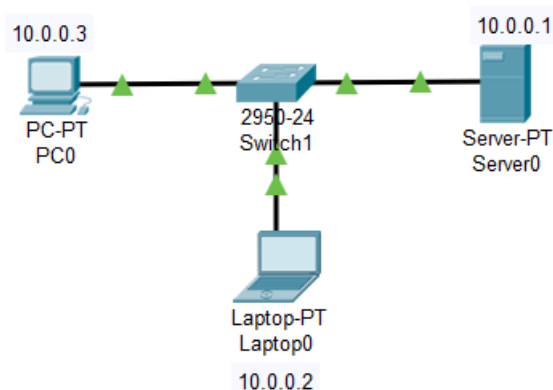
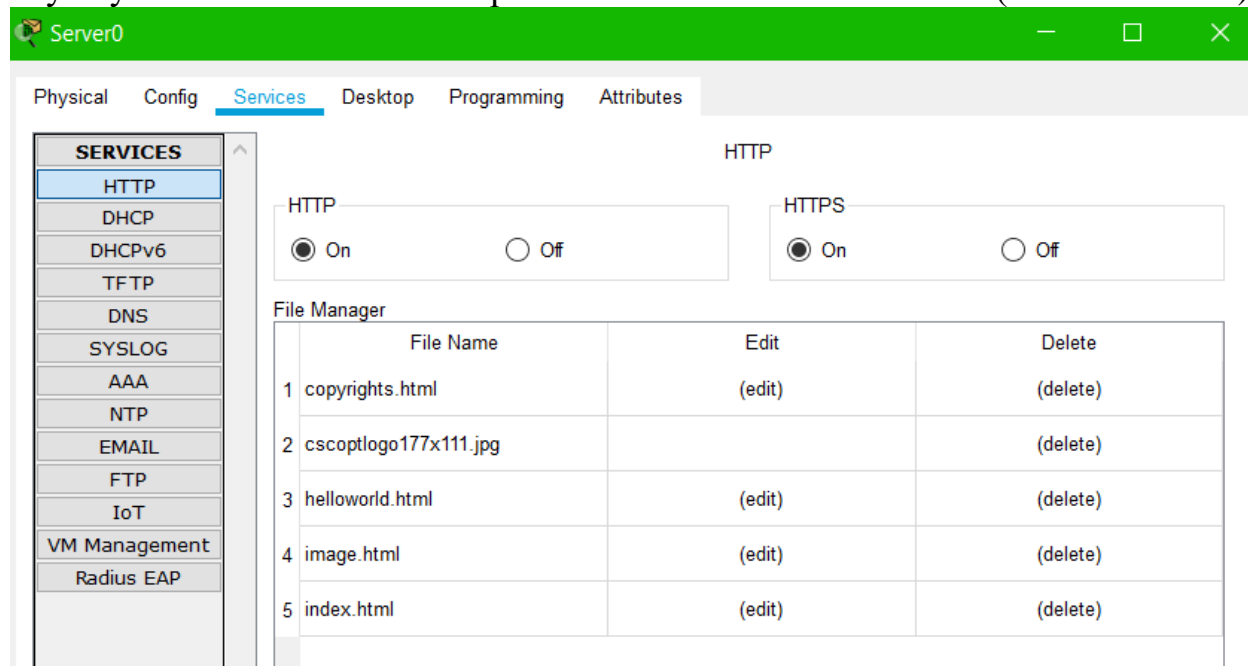


Рис. 5.1. Схема сети

### Создаем WEB-документ на сервере

Для создания HTTP-сервера открываем на сервере вкладку HTTP и редактируем первую страницу сайта с названием **index.html**. Включаем службу HTTP переключателем On (Рис. 5.2).



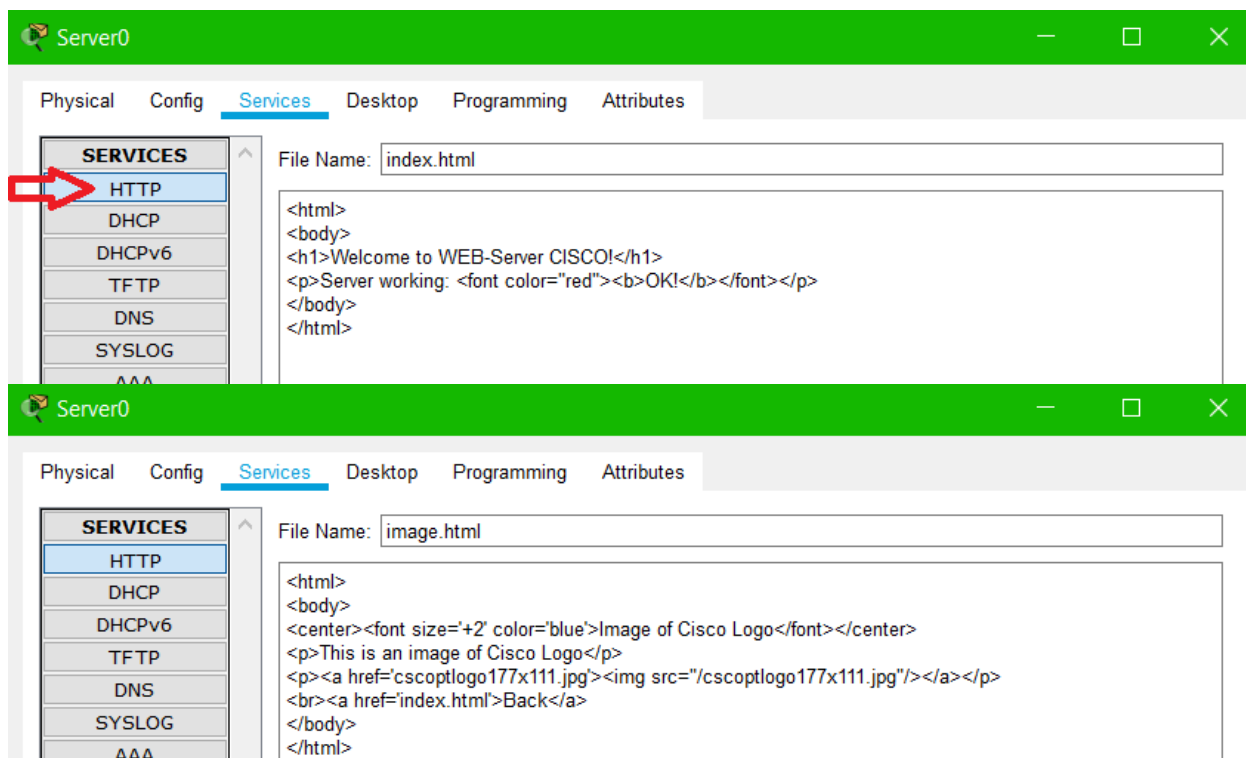
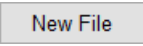



Рис. 5.2. Вкладка Config, служба сервера HTTP

### Примечание

В этом окне можно добавить новую страницу кнопкой  или удалить текущую кнопкой 

В окне html кода создаем текст первой страницы сайта **index.html**. Вариант 1 (Рис. 5.3).

```
<html>
<body>
<h1>Welcome to WEB-Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

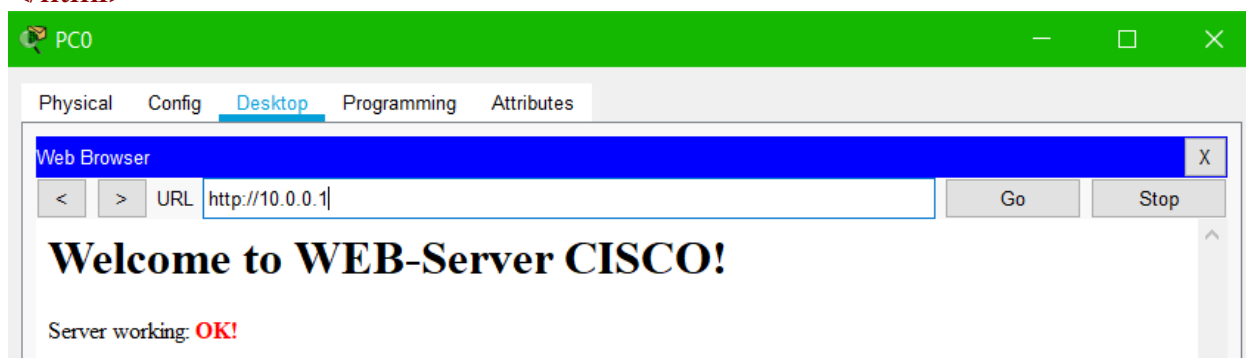


Рис. 5.3. Текст web-страницы, вариант 1

Либо вариант 2 (рис. 5.4)

```
<html>
<center><font size='+2' color='blue'>Welcome to Cisco Packet Tracer HTML
Server! </font></center>
<body>
Hello!<br/>I am OK!
</body>
</html>
```

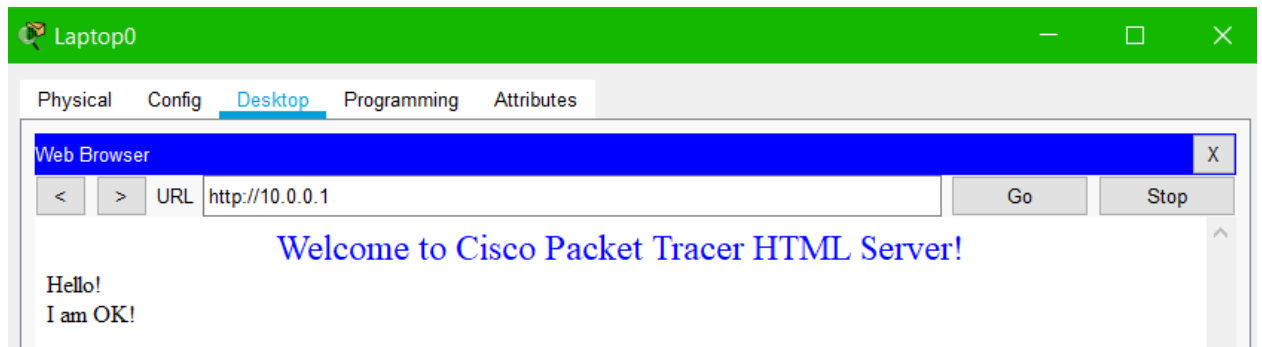


Рис. 5.4. Текст web-страницы, вариант 2

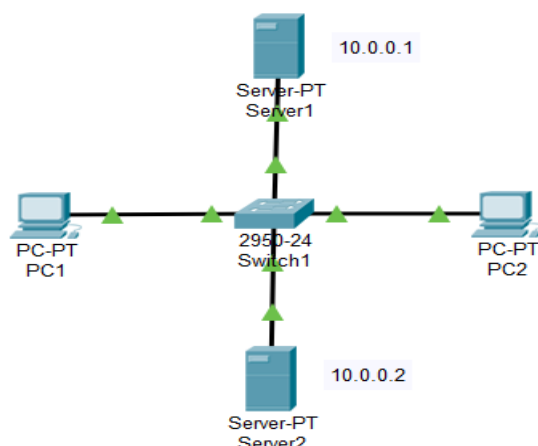
### Совет

Текст можно переносить в это окно через буфер обмена. Он может быть только на английском языке

Для того, чтобы проверить работоспособность нашего сервера, открываем клиентскую машину (10.0.0.2 или 10.0.0.3) и на вкладке **Desktop** (Рабочий стол) запускаем приложение **WebBrowser**. После чего набираем адрес нашего WEB-сервера 10.0.0.1 и нажимаем на кнопку **GO**. Убеждаемся, что наш веб-сервер работает.

## Практическая работа 5-1. Настройка сетевых сервисов DNS, DHCP и Web

Создайте схему сети, представленную на рис. 5.5.

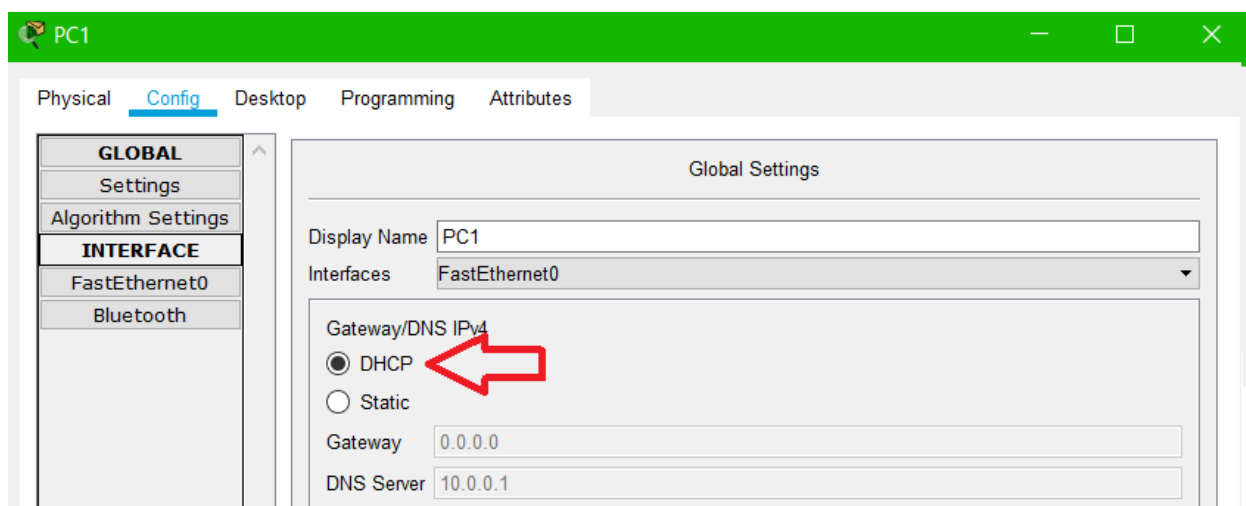


**Рис. 5.5.** Схема сети

Наша задача состоит в том, чтобы настроить Server1 как *DNS* и *Web-сервер*, а Server2 как *DHCP сервер*. Напомню, что работа *DNS* - сервера заключается в преобразовании доменных имен серверов в *IP*-адреса. *DHCP сервер* позволяет организовывать пулы для автоматического конфигурирования сетевых интерфейсов, то есть, обеспечивает автоматическое распределение *IP*-адресов между компьютерами в сети. Иначе говоря, в нашем случае компьютеры получают *IP*-адреса благодаря сервису *DHCP* Server2 и открывают, например, *сайт* на Server1.

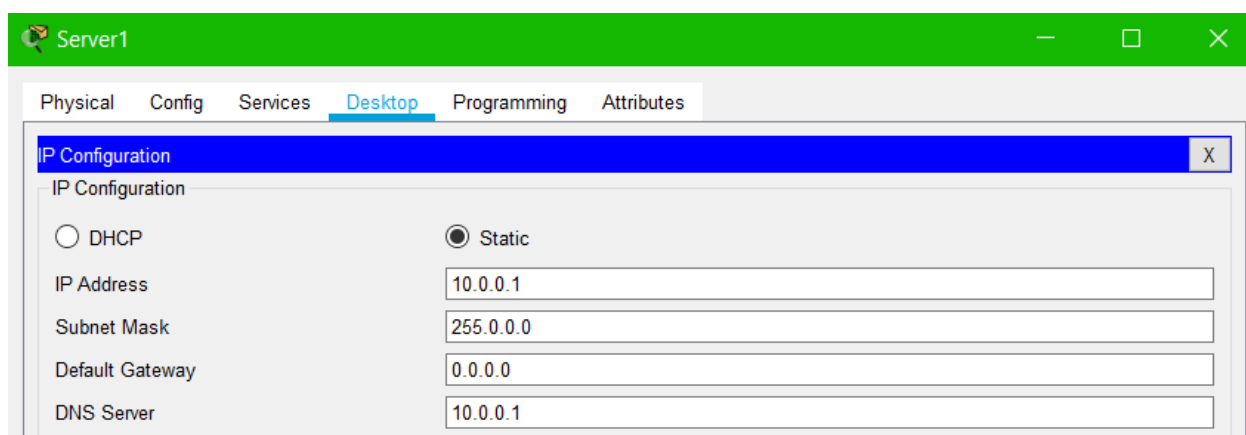
### Настраиваем IP адреса серверов и DHCP на ПК

Войдите в конфигурацию PC1 и PC2 и установите настройку IP через DHCP сервер рис. 5.6.

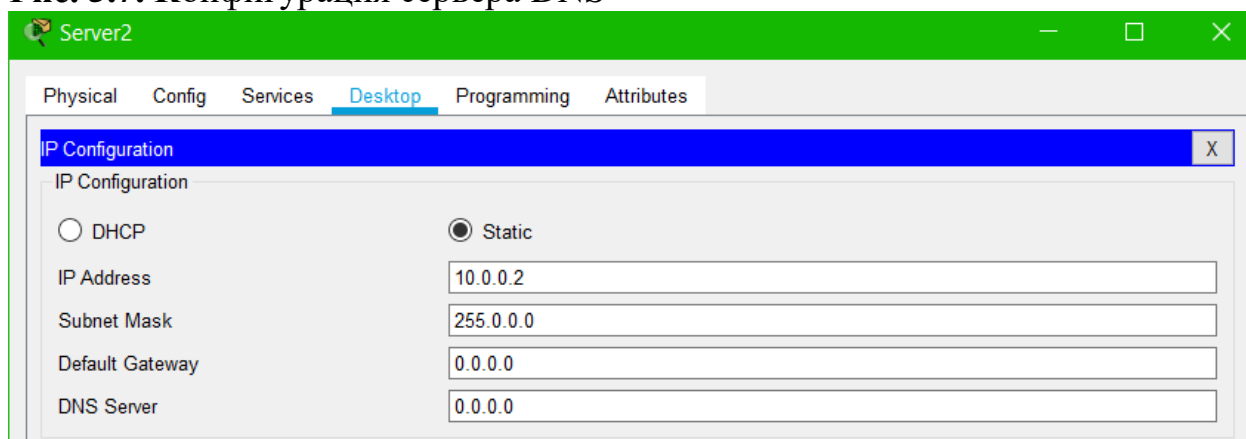


**Рис. 5.6.** Настройка IP на PC1

Задайте в конфигурации серверов настройки IP: Server1 – 10.0.0.1 (Рис. 5.7), Server2 – 10.0.0.2 (рис. 5.8) Маска подсети установится автоматически как 255.0.0.0.



**Рис. 5.7.** Конфигурация сервера DNS



**Рис. 5.8.** Конфигурация сервера DHCP

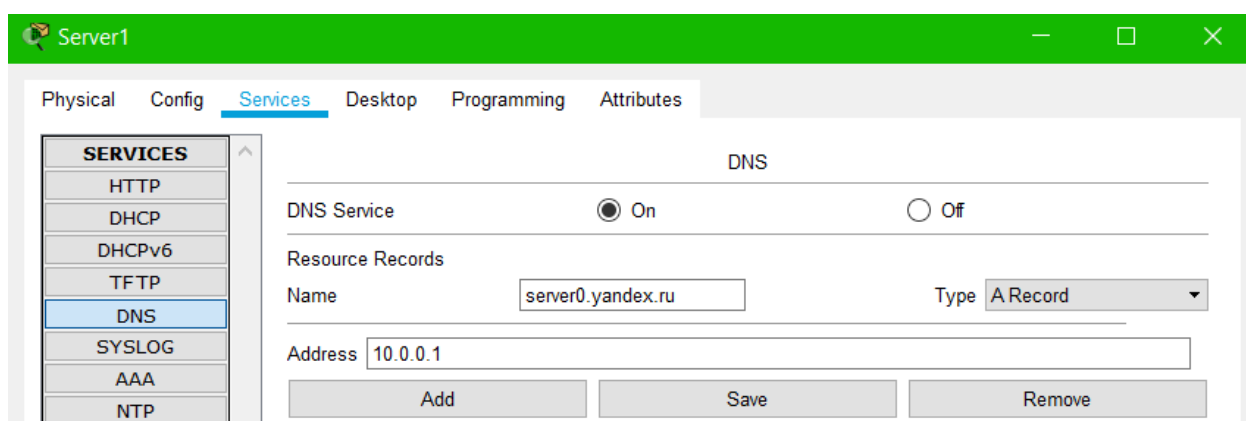
### Настройка служб DNS и HTTP на Server1

В конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи (Resource Records) в прямой зоне DNS.

#### Новый термин

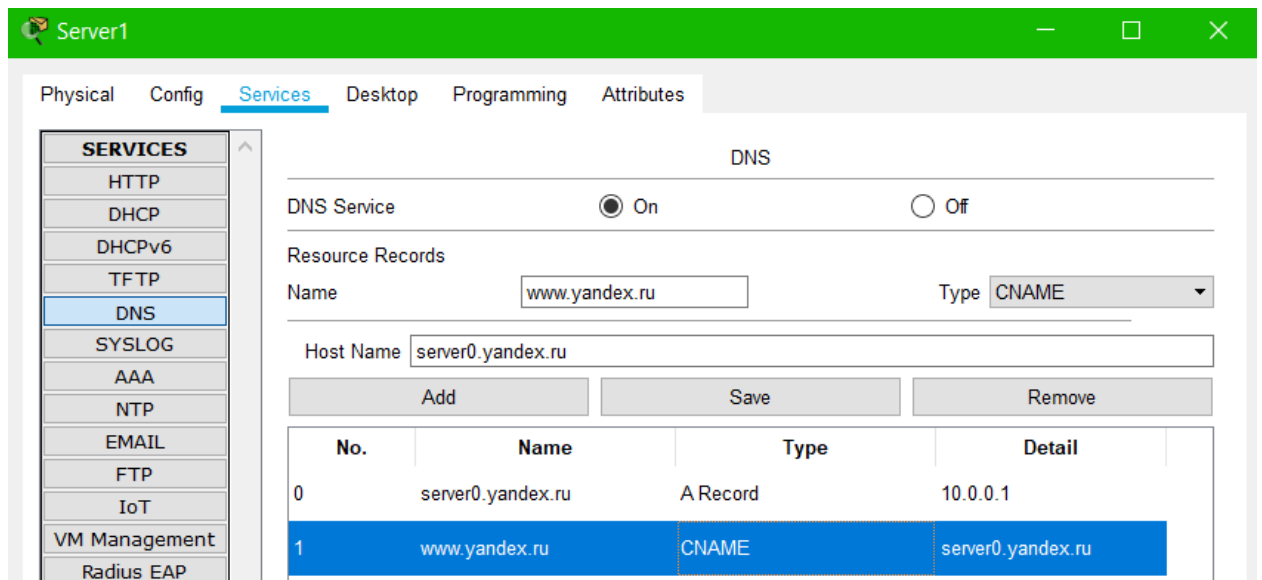
**Зона DNS** — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на сервере доменных имен (DNS-сервере). В зоне прямого просмотра на запрос доменного имени идет ответ в виде IP адреса. В зоне обратного просмотра по IP мы узнаем доменное имя ПК.

Сначала в ресурсной записи типа **A Record** свяжите доменное имя компьютера **server1.yandex.ru** с его IP адресом **10.0.0.1** и нажмите на кнопку **Add** (добавить) и активируйте переключатель **On** Рис. 5.9.



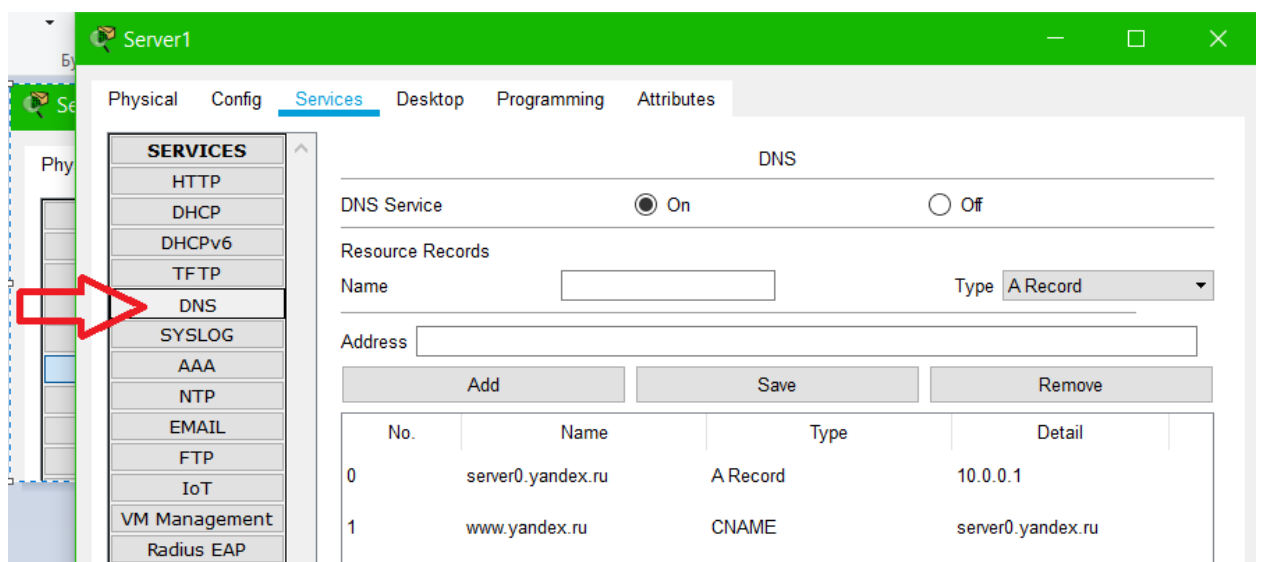
**Рис. 5.9.** Ввод ресурсной записи типа A Record

Далее в ресурсной записи типа **CNAME** свяжите название сайта с сервером и нажмите на кнопку **Add** (добавить) – Рис. 5.10.



**Рис. 5.10.** Ввод ресурсной записи типа CNAME

В результате должно получиться следующее (Рис. 5.11).



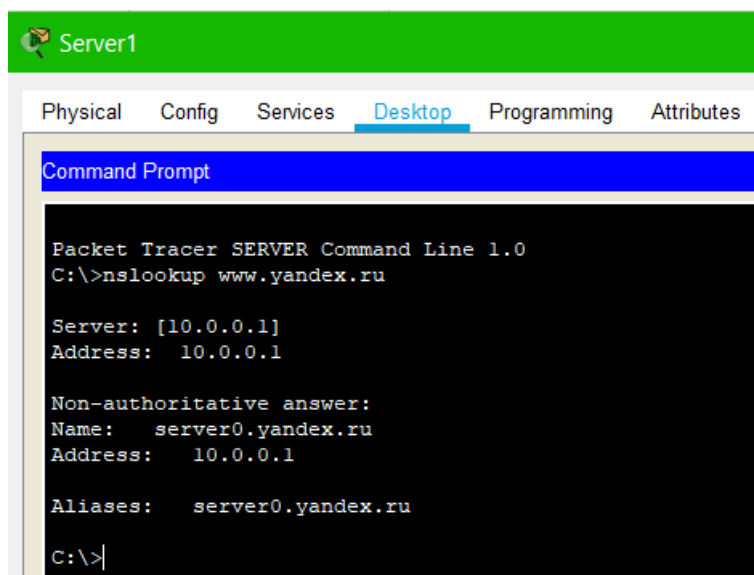
**Рис. 5.11.** Служба DNS в прямой зоне

Теперь настроим службу HTTP. В конфигурации Server1 войдите на вкладку HTTP и создайте стартовую страницу сайта (Рис. 5.12).

```
<html>
<center><font size='+2' color='green'>Web Server</font></center>
www.yandex.ru
<p>
Hello!<br/>I am Server1
</html>
```

### Рис. 5.12. Стартовая страница сайта

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки правильности работы прямой зоны DNS сервера введите команду **SERVER>nslookup** . Если все правильно настроено, то вы получите отклик на запрос с указанием доменного имени DNS сервера в сети и его IP адреса (Рис. 5.13).



### Рис. 5.13. Служба DNS в прямой зоне DNS на Server1 настроена правильно

#### Примечание

Команда **nslookup** служит для определения ip-адреса по доменному имени (и наоборот).

### Настройка службы DHCP на Server2

Войдите в конфигурацию Server2 и на вкладке DHCP настройте службу DHCP. Для этого наберите новые значения пула, установите переключатель **On** и нажмите на кнопку **Save** (Сохранить) – рис. 5.14.

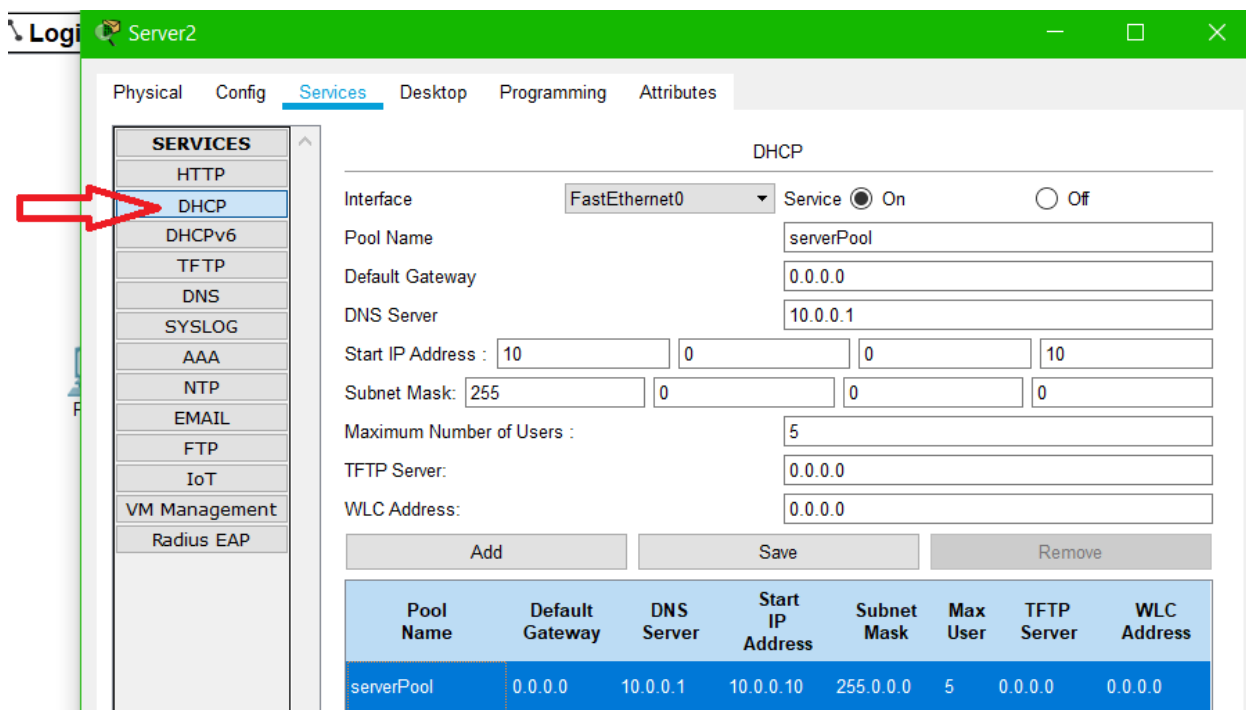


Рис. 5.14. Настройка DHCP сервера.

### Проверка работы клиентов

Войдите в конфигурации хоста PC1 и PC2 и в командной строке сконфигурируйте протокол TCP/IP. Для этого командой **PC>ipconfig /release** сбросьте (очистите) старые параметры IP адреса (Рис. 5.15).

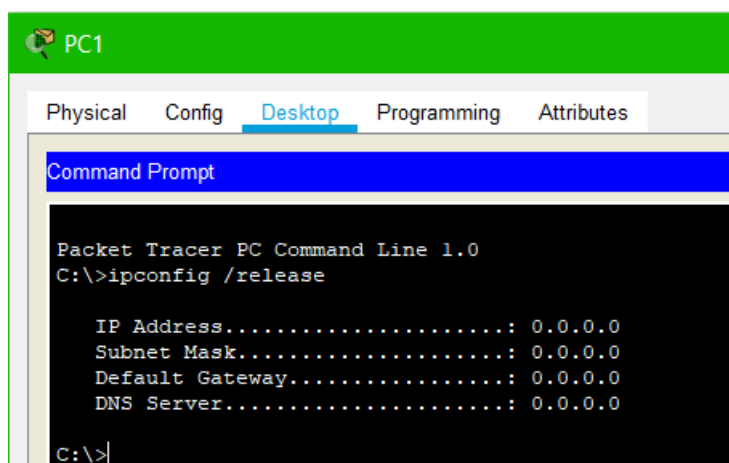


Рис. 5.15. Удаление конфигурации IP-адресов для всех адаптеров

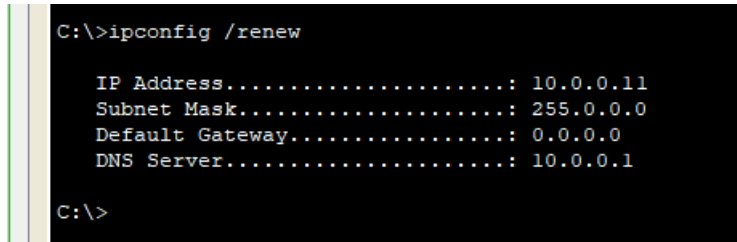
### Примечание

Команда **ipconfig /release** отправляет сообщение **DHCP RELEASE** серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан). Этот



ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

Теперь командой **PC>ipconfig /renew** получите новые параметры от DHCP сервера (Рис. 5.16).



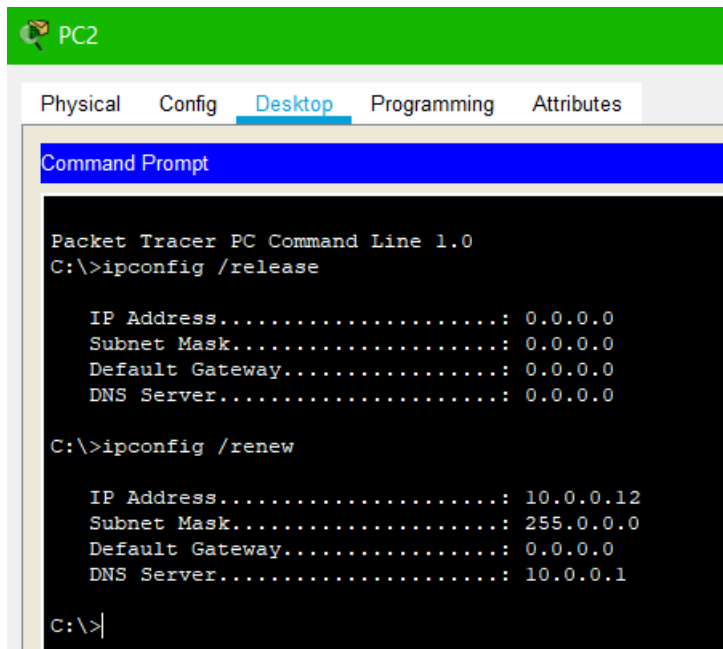
```
C:\>ipconfig /renew

IP Address.....: 10.0.0.11
Subnet Mask.....: 255.0.0.0
Default Gateway...: 0.0.0.0
DNS Server.....: 10.0.0.1

C:\>
```

**Рис. 5.16.** Конфигурация протокол TCP/IP клиента от DHCP сервера

Аналогично поступите для PC2 (рис 5.17).



```
PC2

Physical  Config  Desktop  Programming  Attributes

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ipconfig /release

IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway...: 0.0.0.0
DNS Server.....: 0.0.0.0

C:\>ipconfig /renew

IP Address.....: 10.0.0.12
Subnet Mask.....: 255.0.0.0
Default Gateway...: 0.0.0.0
DNS Server.....: 10.0.0.1

C:\>|
```

**Рис. 5.17.** PC2 получил IP адрес от DHCP сервера Server2

Осталось проверить работу WEB сервера Server1 и открыть сайт в браузере на PC1 или PC2 (Рис. 5.18).

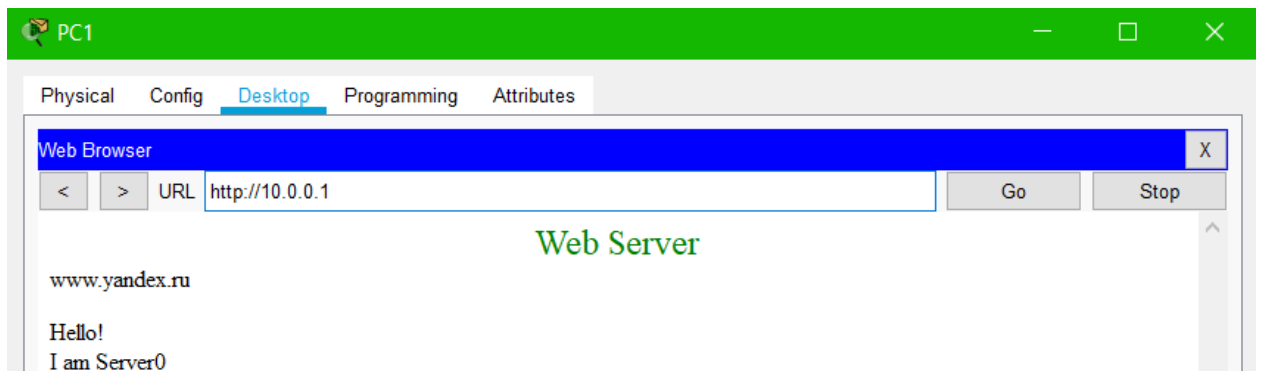


Рис. 5.18. Проверка работы службы HTTP на Server1

## Примеры работы маршрутизатора в роли DHCP сервера

*Маршрутизация (routing)* – процесс определения маршрута следования информации в сетях связи. Задача маршрутизации состоит в определении последовательности транзитных узлов для передачи пакета от источника до адресата. *Определение* маршрута следования и продвижение *IP*-пакетов выполняют специализированные сетевые устройства – маршрутизаторы. Каждый *маршрутизатор* имеет от двух и более сетевых интерфейсов, к которым подключены: *локальные сети* либо маршрутизаторы соседних сетей.

### Новый термин

*Маршрутизатор (router, роутер)* – сетевое устройство третьего уровня модели OSI, обладающее как минимум двумя сетевыми интерфейсами, которые находятся в разных сетях. Маршрутизатор может иметь интерфейсы: для работы по медному кабелю, оптическому кабелю, так и по беспроводным "линиям" связи.

Выбор маршрута *маршрутизатор* осуществляет на основе таблицы маршрутизации. Таблицы маршрутизации содержат информацию о сетях, и интерфейсов, через которые осуществляется подключение непосредственно, а также содержатся сведения о маршрутах или путях, по которым *маршрутизатор* связывается с удаленными сетями, не подключенными к нему напрямую. Эти маршруты могут назначаться администратором статически или определяться динамически при помощи программного протокола маршрутизации. *Таблица* маршрутизации содержит набор правил – записей, состоящих из определенных полей. Каждое правило содержит следующие основные поля-компоненты:

- адрес IP-сети получателя,
- маску,
- адрес следующего узла, которому следует передавать пакеты,

- административное расстояние — степень доверия к источнику маршрута,
- метрику - некоторый вес - стоимость маршрута,
- интерфейс, через который будут продвигаться данные.

Пример таблицы маршрутизации:

```
192.168.64.0/16 [110/49] via 192.168.1.2, 00:34:34, FastEthernet0/0.1
```

где 192.168.64.0/16 – сеть назначения,  
 110/- административное расстояние  
 /49 – метрика маршрута,  
 192.168.1.2 – адрес следующего маршрутизатора, которому следует  
 передавать пакеты для сети 192.168.64.0/16,  
 00:34:34 – время, в течение которого был известен этот маршрут,  
 FastEthernet0/0.1 – интерфейс маршрутизатора, через который можно  
 достичь «соседа» 192.168.1.2.

Протокол *DHCP* представляет собой *стандартный протокол*, который позволяет серверу динамически присваивать клиентам *IP*-адреса и сведения о конфигурации. Идея работы *DHCP* сервиса такова: на ПК заданы настройки получения *ip* адреса автоматически. После включения и загрузки каждый ПК отправляет широковещательный *запрос* в своей сети с вопросом "Есть здесь *DHCP сервер* - мне нужен *ip адрес*?". Данный *запрос* получают все компьютеры в подсети, но ответит на этот *запрос* только *DHCP сервер*, который отправит компьютеру свободный *ip адрес* из пула, а также маску и *адрес* шлюза по умолчанию. *Компьютер* получает параметры от *DHCP* сервера и применяет их. После перезагрузки ПК снова отправляет широковещательный *запрос* и может получить другой *ip адрес* (первый свободный который найдется в пуле адресов на *DHCP* сервере).

*Маршрутизатор* можно сконфигурировать как *DHCP сервер*. Иначе говоря, вы можете программировать *интерфейс* маршрутизатора на раздачу настроек для хостов.

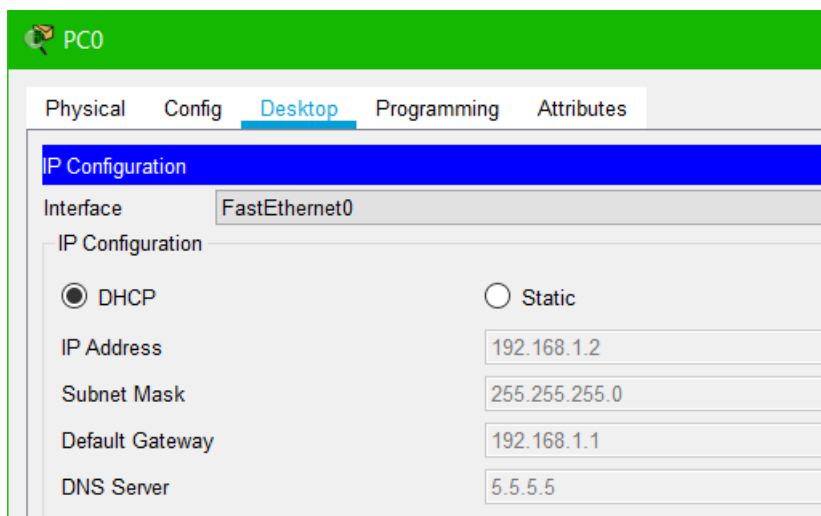
Системный *администратор* настраивает на сервере *DHCP* параметры, которые передаются клиенту. Как правило, *сервер DHCP* предоставляет клиентам по меньшей мере: *IP-адрес*, маску подсети и основной *шлюз*. Однако предоставляются и дополнительные сведения, такие, например, как *адрес* сервера *DNS*.

## Практическая работа 5-2. Конфигурирование DHCP сервера на маршрутизаторе

Схема сети приведена на рис. 5.19. С помощью настроек ПК, представленных на рисунке, мы указываем хосту, что он должен получать *IP адрес*, *адрес* основного шлюза и *адрес DNS* сервера от *DHCP* сервера.

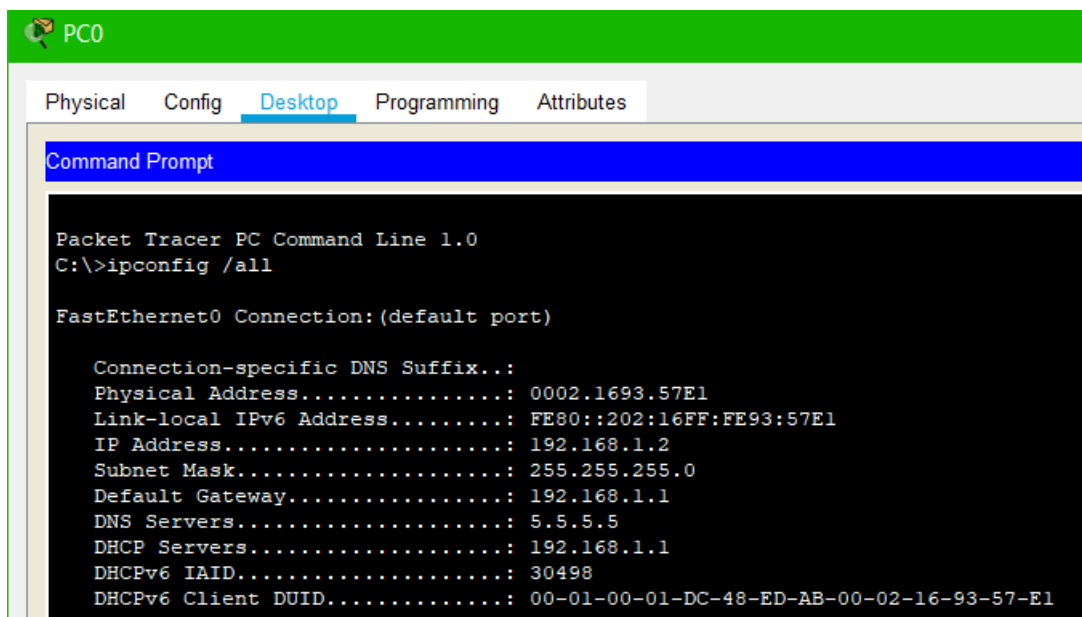


Проверим результат получения динамических параметров для PC0 (рис. 5.21).



**Рис. 5.21.** DHCP работает

Проверим работоспособность *DHCP* сервера на хосте PC0 командой **ipconfig /all** (Рис. 5.22).

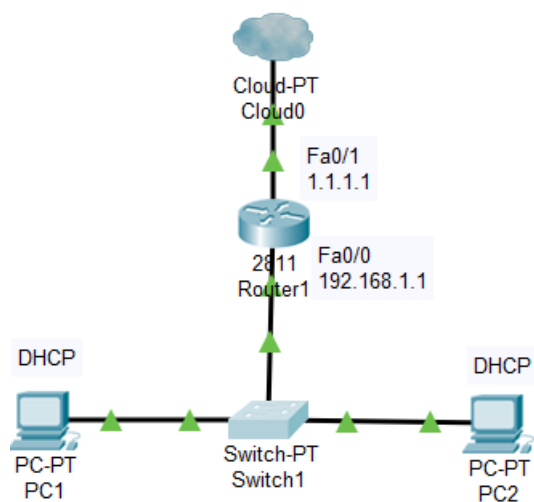


**Рис. 5.22.** Хост получил настройки от DHCP сервера

Хост успешно получил *IP* адрес, адрес шлюза и адрес *DNS* сервера от *DHCP* сервера R0.

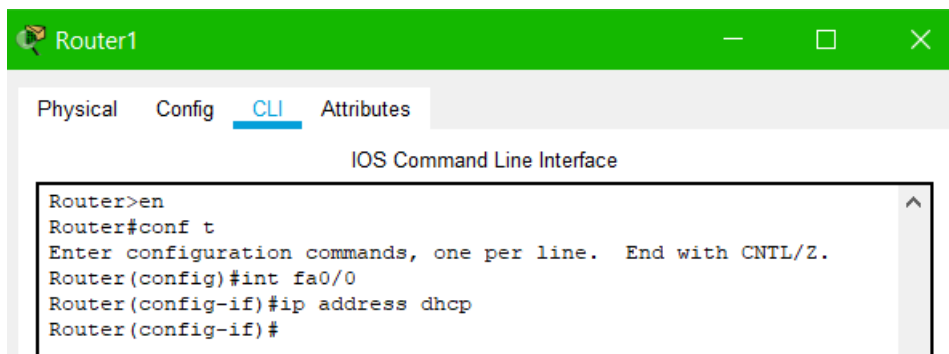
### Практическая работа 5-3. Пример настройки интерфейса маршрутизатора в качестве DHCP клиента

Схема сети показана на Рис. 5.23.



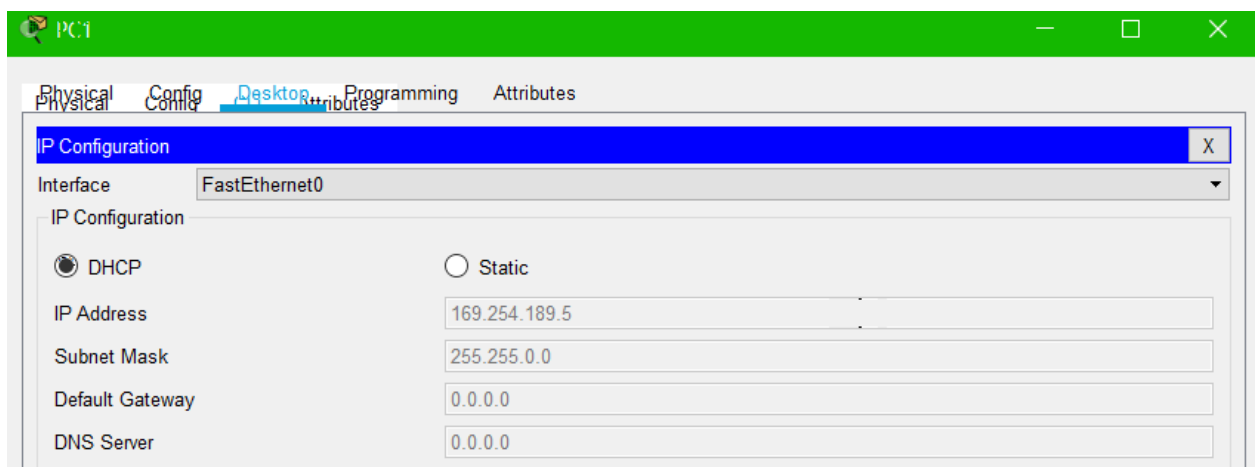
**Рис. 5.23.** Схема сети

Конфигурируем *интерфейс* Fa0/0 для R1 (Рис. 5.24).



**Рис. 5.24.** Конфигурируем интерфейс маршрутизатора

Наблюдаем результат (Рис. 5.25).



**Рис. 5.25.** DHCP не работает

После настройки интерфейса роутера на получение настроек по *DHCP*, *DHCP* клиент на PC1 перестал получать *IP-адрес* – *IP* из диапазона **169.254.x.x/16** назначается автоматически самим ПК при проблемах с получением адреса по *DHCP*. Интерфейс роутера *IP-адрес* так же не получит т.к. в данной подсети нет *DHCP* серверов.

### Практическая работа 5-4. DHCP сервер на маршрутизаторе

В этом примере мы будем конфигурировать маршрутизатор 285, а именно, настраивать на нем *DHCP сервер*, который будет выдавать по *DHCP* адреса из сети 192.168.1.0 (Рис. 5.26). PC1 и PC2 будут получать настройки динамически, а для сервера желательно иметь постоянный *адрес*, т.е., когда он задан статически.

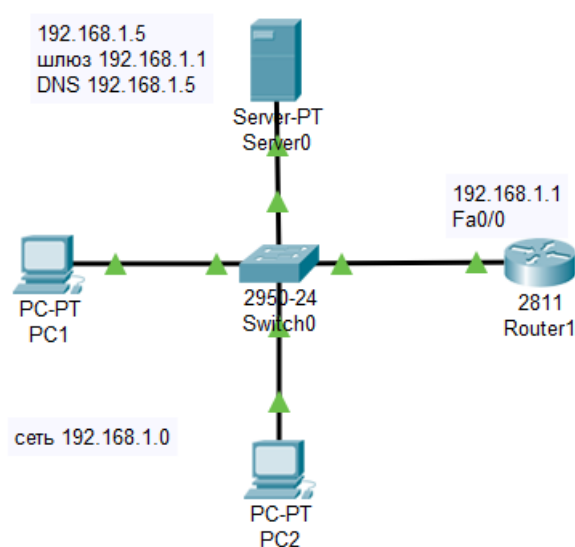


Рис. 5.26. Схема сети

#### Примечание

Как устройство с постоянным адресом здесь можно включить еще и принтер.

#### Резервируем 10 адресов

```
R1 (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

#### Примечание

Этой командой мы обязали маршрутизатор R1 не выдавать адреса с 192.168.1.1 по 192.168.1.10 потому, что адрес 192.168.1.1 будет использоваться самим маршрутизатором как шлюз, а остальные адреса мы зарезервируем под различные хосты этой сети.

Таким образом, первый *DHCP адрес*, который выдаст R1 равен **192.168.1.11**.

#### Создаем пул адресов, которые будут выдаваться из сети 192.168.1.0

```
R1 (config)#ip dhcp pool POOL1
```

```
R1 (dhcp-config)#network 192.168.1.0 255.255.255.0
R1 (dhcp-config)#default-router 192.168.1.1
R1 (dhcp-config)#domain-name my-domain.com
R1 (dhcp-config)#dns-server 192.168.1.5
```

### Примечание

Согласно этим настройкам выдавать адреса из сети 192.168.1.0 (кроме тех, что мы исключили) будет маршрутизатор R1 через шлюз 192.168.1.1.

### Настраиваем интерфейс маршрутизатора

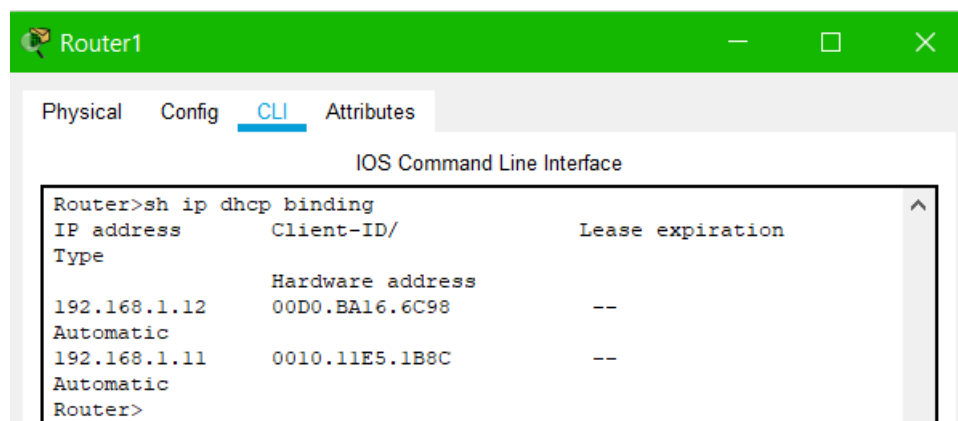
```
R1 (config)#interface fa0/0
R1 (config-if)#ip address 192.168.1.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1(config)#exit
R1#
```

### Примечание

Команда **no shut** (сокращение от noshutdown) используется для того, чтобы бы интерфейс был **активным**. Обратная команда – shut, выключит интерфейс.

### Проверка результата

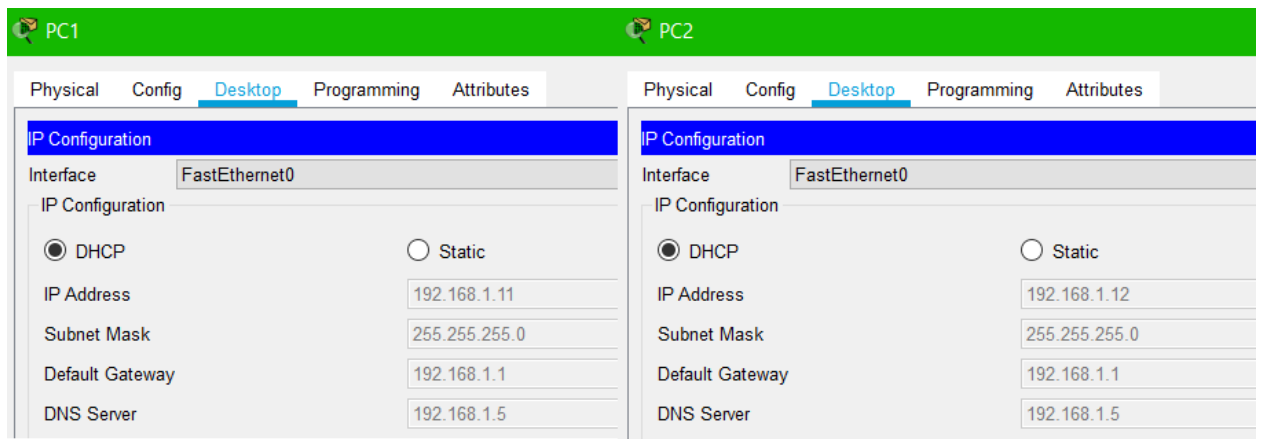
Теперь оба ПК получили настройки и командой **R1#show ip dhcp binding** можно посмотреть на *список* выданных роутером адресов (Рис. 5.27).



**Рис. 5.27.** Адреса выдаются автоматически, начиная с адреса 192.168.1.5

Итак, мы видим, что протокол *DHCP* позволяет производить автоматическую настройку сети на всех компьютерах (Рис. 5.28).





**Рис. 5.28.** PC1 и PC2 получают IP адреса от DHCP сервера

### Подготовить отчет по выполненным заданиям:

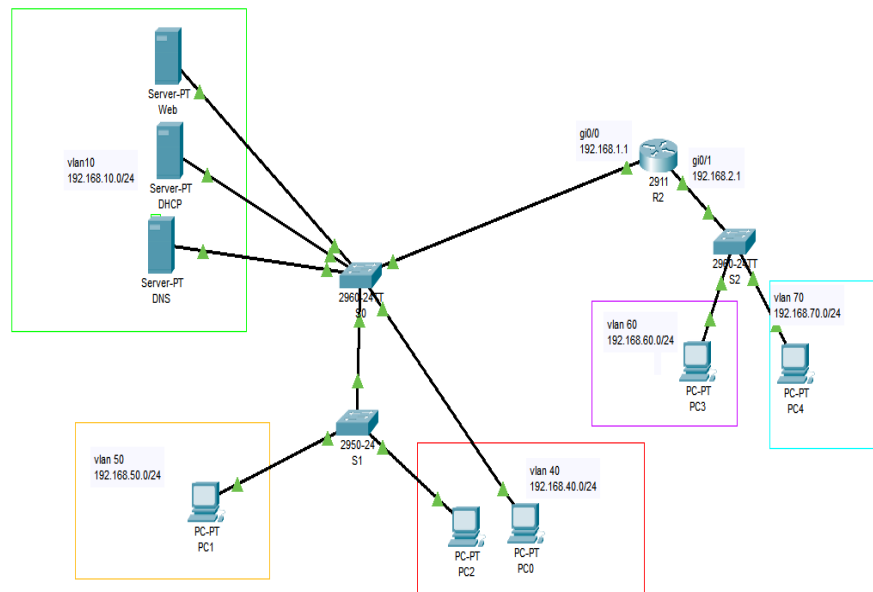
1. Цель работы
2. Топология созданной сети
3. Что настроено
4. Проверка работоспособности
5. Ответить на вопросы

### Вопросы:

1. Что такое рекурсивный запрос DNS и какова схема его работы?
2. Зачем нужен DNS протокол?
3. Виды записей DNS.
4. Зачем нужна обратная зона DNS?
5. Какими сообщениями обмениваются клиент и сервер DHCP?
6. В чем различие динамического и автоматического методов назначения адресов IPv4?
7. Каково назначение команды *Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.5*?
8. Каково назначение команды *Router(config)#ip dhcp pool SERV-DH*. В какой режим при этом переходит маршрутизатор?
9. Какую команду нужно дать, чтобы маршрутизатор получал IP-адреса от сервера DHCP?
10. Какая команда позволяет клиенту получать адресную информацию от DHCP-сервера, расположенного в другой локальной сети?

11. Как настраивается пул адресов DHCP?
12. Какие параметры получает хост от DHCP сервера?
13. Приведите команды для настройки сетевого интерфейса роутера.
14. Какой командой можно посмотреть текущие настройки роутера?
15. Как просмотреть настройки свитча?
16. Какая команда существует для просмотра таблицы продвижения на свитче?

## Практическая работа №12 Самостоятельная работа



### Задание для самостоятельной работы:

1. Реализовать сеть, разделенную на 5 vlan: 10, 40, 50, 60 и 70.
2. Настроить VTP на Switch0, Switch1.
3. VLAN 10 должна быть доступна из любой другой vlan, в ней находятся все серверы.
4. Конечные узлы других vlan не должны иметь возможности взаимодействовать между собой.
5. Во vlan 10 реализовать:
  - Web сервер. Создайте на нем страницу index.html с текстом «I ( your name) AM SUPER»:

- DNS сервер содержит доменную запись «super.ru», указывающую на Web сервер.
  - DHCP сервер содержит пулы адресов для отдельной подсети каждой vlan.
6. DHCP раздает адреса во все подсети (в каждую vlan). Из каждого пула адресов (определенной VLAN) исключить первые пять адресов.

Так как маршрутизатор подключен к центральному коммутатору, то интерфейсы у нас будут не физические, а виртуальные - подинтерфейсы. Для этого следует сконфигурировать на интерфейсе роутера виртуальные подинтерфейсы для работы с vlan.

#### **Пример:**

Создадим на интерфейсе fa0/0 подинтерфейсы. Каждый из подинтерфейсов будет иметь собственный IP-адрес, соответствующий определенной VLAN.

```
R1(config)#int f0/0.10      {Создание подинтерфейса}
R1(config-subif)#encapsulation dot1Q 10    {определение номера виртуальной сети}
R1(config-subif)#ip address 10.10.0.1 255.255.255.0 {адрес подинтерфейса}
R1(config-subif)# ip access-group 10 out    {Привязка списка доступа к интерфейсу}
```

```
R1(config)#int f0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.20.0.1 255.255.255.0
R1(config-subif)# ip access-group 20 out
```

```
R1(config)#int f0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.30.0.1 255.255.255.0
R1(config-subif)#ip access-group 30 out
```

Обратите внимание на команду encapsulation. Она определяет номер виртуальной сети, в которой будет находиться данный подинтерфейс.

*Не забудьте создать транковый порт на свитче для связи с роутером!*

На каждом подинтерфейсе назначается список доступа - access list (ACL) с номером, соответствующим номеру vlan. В этих ACL будут впоследствии сконфигурированы правила доступа к подсетям.

Стандартный список доступа:

```
Router(config)#access-list {номер} {permit или deny} {адрес источника}
```

На роутере настроить соответствующие списки доступа.

Пример:

```
access-list 40 deny 192.168.50.0 0.0.0.255
access-list 40 deny 192.168.60.0 0.0.0.255
access-list 40 deny 192.168.70.0 0.0.0.255
access-list 40 permit any
access-list 50 deny 192.168.40.0 0.0.0.255
access-list 50 deny 192.168.60.0 0.0.0.255
access-list 50 deny 192.168.70.0 0.0.0.255
```

Для выполнения задачи каждый список будет содержать набор правил, запрещающий пропускать пакеты подсети любого vlan, кроме vlan, для которой конфигурируется этот список, и vlan 10, которая должен иметь доступ ко всем остальным. Другие пакеты будут разрешены. Таким образом гарантирована возможность обмена данных с внешней сетью.

7. Для всех подинтерфейсов, кроме предназначенного для vlan 10, настроить 192.168.10.2 как DHCP relay (использовать команду *helper address*). По данному адресу будет располагаться DHCP сервер, поэтому широковещательные DHCP запросы из подсетей транслируются на DHCP сервер (см. пример в приложении 1).

8. Для DHCP сервера использовать доверенный порт.

9. Все устройства в сети должны иметь параметры Display name и Host name, соответствующие фамилии+имени выполнившего работу студента.

Для успешного выполнения практических работ можно воспользоваться следующими ресурсами:

1. Сети для самых маленьких <https://linkmeup.ru/blog/588/>

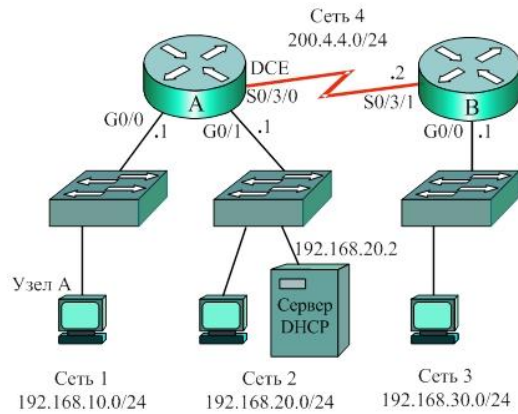
2. Курс молодого бойца <https://www.youtube.com/playlist?list=PLArYZbSM72P9FinOb0P9S4NiRyaz-zLJN>

3. Книга «Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание» <https://www.rulit.me/author/olifer-v-g/kompyuternye-seti-principy-tehnologii-protokoly-5-e-izdanie-download-475363.html>

## Приложение 1

Общие сведения о динамическом конфигурировании узлов  
Ретрансляция сообщений DHCP

Во многих случаях клиент и DHCP-сервер могут находиться в разных сетях, например, узел А (рис.1) находится в сети 1, а сервер - в сети 2.



**Рис. 1.** Ретрансляция DHCP

Конфигурирование функции ретрансляции разрешает маршрутизатору пересылать широковещательные сообщения DHCP-протокола. Для этого на интерфейсе G0/0 маршрутизатора R-A конфигурируется команда с адресом DHCP-сервера:

```
R-A(config)#int g0/0
```

```
R-A(config-if)#ip helper-address 192.168.20.2
```

В этом случае маршрутизатор выступает в роли ретранслятора. Он получает от узла А широковещательные запросы (DHCP DISCOVER, DHCP REQUEST) и пересылает их на уникальный адрес (192.168.20.2) DHCP-сервера, который выделяет адреса узлу А.